Artículo original

Ciberdefensa como estrategia para la seguridad y soberanía digital en Paraguay
Cyberdefense as a strategy for security and digital sovereignty in Paraguay
Ciberdefensa jeporukuaa omombarete haguã pe seguridad ha soberanía Digital Paraguáipe

*Alfredo Jonás Ramírez
https://orcid.org/0000-0001-9407-1069
Ministerio de Defensa. Asunción, Paraguay

Resumen

Este artículo aborda la temática de la política de ciberdefensa, que debe contribuir a la Defensa Nacional del ciberespacio. En un mundo altamente interconectado, esta estrategia se erige como una pieza fundamental para resguardar la seguridad y soberanía digital de una nación. Al integrarse como política de Defensa Nacional año 2019 - 2030, esta disciplina busca enfrentar los desafíos emergentes en el ciberespacio, protegiendo sistemas críticos de posibles ataques maliciosos. La metodología es de enfoque cualitativo, con un diseño no experimental de tipo documental, considerando que está basada en consultas de fuentes bibliográficas y análisis de teorías y prácticas, garantiza que el artículo cuente con sólidas evidencias y perspectivas informadas. Como técnica de recolección de datos se utilizó el análisis documental logrando de esta manera

Recibido: 11/08/23 Aprobado: 12/12/23

*Sub Director General de la dirección general de Tecnología de la Información y Comunicación. Fuerzas Armadas de la Nación. Asunción, Paraguay. Email: ramirezjonasalfredo@gmail.com

Máster en Política y Estrategia Aeroespacial (CIAERE- 2021); Magíster en Ciencias Militares (ECEME 2017); Máster en Operaciones Militares (EPOE 2009); Post Grado en Didáctica Superior (CIMEE/CCPC 2005). Grado: Lic. Ciencias Militares (ACADEMIL 1995); Lic. en Relaciones Internacionales (UNIDA – 2020). Especialista en Metodología de la Investigación Científica (CIMEE/CCPC 2021); Especialista en Ciberdefensa y Ciberseguridad Estratégica (IAEE 2020); Programa de Capacitación en Ciberseguridad (UNIDA 2020); Diplomado en Defensa y Desarrollo Nacional (UNIGRAN 2020); Tutoría de Tesis (IAEE/CCPC 2018); Programa de Capacitación en Liderazgo Estratégico (IAEE 2017); Especialista en Inteligencia Estratégica (PEIE/IAEE 2016); Diplomado de Alta Gerencia en Seguridad Centro de Estudios de Seguridad del Perú (CESP 2011); Especialista en Operaciones Psicológicas y Operaciones de información. Escuela de Relaciones Civiles y Militares de Bogotá - Colombia (ERSM-2008).

ISSN 2415-5063 Versión impresa ISSN 2415-5071 Versión en línea
https://ojs.ministeriopublico.gov.py Contacto: dip.informaciones@ministeriopublico.gov.py

un alcance proyectivo. Esto es fundamental para abordar el dinámico y cambiante campo en el que ocurren los ciberataques. En síntesis, se pude afirmar que ambas materias se complementan y convergen para asegurar la seguridad y resiliencia del país en un entorno cibernético en constante evolución.

Palabras claves: Ciberdefensa, Paraguay, política de seguridad, estrategia.

Abstract

This article covers the issue of cyber defense policy, which should contribute to the National Defense of cyberspace. In a highly interconnected world, this strategy stands as a fundamental piece to safeguard the security and digital sovereignty of a nation. When integrated into the National Defense policy for the year 2019 - 2030, this discipline seeks to face the emerging challenges in cyberspace, protecting critical systems from possible malicious attacks. Thus, the methodology is qualitative in approach, with a non-experimental design of documentary type, considering that it is based on consultations of bibliographic sources and analysis of theories and practices, ensuring that the article has solid evidence and informed perspectives. Documentary analysis was used as a data collection technique, thus achieving a projective scope. This is essential to address the dynamic and changing field in which cyber attacks occur. In summary, it can be stated that both subjects complement each other and converge to ensure the country's security and resilience in a constantly evolving cyber environment.

Key words: cyber defense, Paraguay, security policy, National Defense, strategy.

Ñemombyky

Ko tembiapo oñe'ẽ opa hendáicha ciberdefensa jeporu rehe, he'i ikatuha omoirũ Defensa Nacional-pe oñangareko haguã Ciberespacio rehe. Ko mundo-pe ningo ojeiko joajupápe, ko estrategia rupive omombarete kuaa pe seguridad ha avei soberanía digital ko tetãme. Ojegueroike upe Política de Defensa Nacional ary 2019-2030-pe, ko mba'ekuaa ohenonde'ase opaichagua desafío omoheñóiva ko ciberespacio, ikatu ojoko umi sistema ikatúva ogueru mba'e vai. Upéicha rupi kóva oiporu pe metodología hérava enfoque cualitativo ha oñembohape diseño no experimental de tipo documental, oñemopyrenda rupi heta kuatiahaipyre ári, ohesa'ỹijo teoría ha avei práctica, omombe'u ko kuatiañe'ẽ oiko haguã ohesa'ỹijo pypuku ha oipyguarapaite. Dato-kuéra ombyatypa haguã katu oiporu pe técnica hérava análisis documental, ohesa'ỹijopaite, upéicha rupi ojepyso hekopete. Ko mba'e tekotevẽ ojekuaa porã ojejuhu umi ciberataque ojejapóva. Oñembyapu'ávo, ikatu oje'e mokõivéva ojogueraha ha oikepaha ojokuápe oiko haguã pe seguridad ha avei pe resiliencia peteĩ tetã oikémava ohóvo cibernético jeku'e pa'ũme.

Ñe'ẽ tee: Ciberdefensa, Paraguay, Política de seguridad, Tetã Ñangareko, estrategia.

Introducción

Las ciberamenazas y ataques cibernéticos han evolucionado en un ecosistema cada vez más complejo, dinámico, interrelacionado y versátil; tal es así, que los incidentes de seguridad en el ciberespacio trascienden todos los campos de las expresiones del poder nacional e inciden en la soberanía digital, produciendo vulnerabilidad de las infraestructuras críticas.

Internacionalmente, existe un creciente desarrollo en la gestión de riesgos asociados al uso de las tecnologías de la información y comunicación, en adelante TIC y la interacción en el ciberespacio. Desde hace años, muchos países cuentan con estrategias con base en las políticas de ciberdefensa. Asimismo, se puede observar la considerable evolución en lo referente a doctrina, normativas y procedimientos, en los diversos organismos y foros internacionales relacionados al tema.

En ese sentido, Paraguay no cuenta con una política ni doctrina de ciberdefensa desde el enfoque de la Defensa Nacional, por ello, el desafío de la realización de este trabajo es sugerir y proporcionar ideas que orienten a esta acción e implementen las medidas que sean necesarias para proteger la seguridad del ciberespacio, considerando las estrategias orientadas a la prevención y concientización en el ambiente digital son fundamentales. Además, se complementan con el programa de gobierno que tiene un plan de ciberseguridad con sus respectivas acciones o estrategias.

En ese entendimiento, la creciente preocupación en el entorno de la seguridad internacional por el rol fundamental, en el contexto de la Defensa Nacional y su proyección a las expresiones del poder nacional, requieren de políticas relacionadas al tema y su proyección a la soberanía digital, a fin de mitigar las amenazas cibernéticas que provengan desde o a través del ciberespacio.

En dicho contexto, una política y doctrina en la materia sirven de sustento para las estrategias a ser implementadas en el ámbito, describen los objetivos y las directrices para tales acciones.

Considerando estos aspectos surgió como problema ¿Cómo se da la regulación para la implementación de una política de ciberdefensa, como un eje de la política de Defensa Nacional para los años 2019 - 2030?

En esta línea, se formuló como objetivo describir la regulación para la implementación de la política de ciberdefensa, como eje de la política de Defensa Nacional para los años 2019-2030. Esta, posteriormente, será presentada desde un ámbito natural de ejecución de la Defensa Nacional; las Fuerzas Militares, en adelante FFMM, instancia que se erige como el órgano de aplicación y ejecución de la materia conforme a la Resolución n.° 573/21 del Ministerio Defensa Nacional, en adelante MDN.

Aspectos Teóricos

Generalidades

La Defensa Nacional es el conjunto de previsiones y acciones que adopta el gobierno para permitir la supervivencia y permanencia del Estado, posibilitando que el proceso de desarrollo se realice en las mejores condiciones de modo a permitir que se pueda alcanzar y mantener los objetivos nacionales. Este es el medio para alcanzar la seguridad integral.

Al respecto, la Constitución Nacional (1992) en el art. 30 «de las señales de comunicación electromagnética», menciona que:

> La emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la soberanía nacional, promoverá el pleno empleo de las mismas según los derechos propios de la República y conforme con los convenios internacionales ratificados sobre la materia.

En efecto, la Política de Defensa Nacional 2019 - 2030, elaborada por el MDN hace referencia a los ataques cibernéticos, de la siguiente manera:

> Ante la necesidad de prevenir y combatir eficientemente las nuevas amenazas; tales como el terrorismo, los secuestros, el crimen organizado transnacional, el narcotráfico, los grupos armados ilegales, los ataques cibernéticos, entre otras; sin descuidar las amenazas tradicionales para la República del Paraguay (s/ n).

De la misma forma, se establece en su apartado VI «Delineamientos Estratégicos para la Defensa», en el punto 6 «de previsión y prospección», referente a considerar y trabajar acerca de las oportunidades y riesgos inexplorados o escasamente desarrollados, para la protección y explotación del ciberespacio y su soberanía.

Así también, en su apartado VIII «Líneas de acción para la defensa» en el punto 1 menciona instituciones con responsabilidades primarias tales como; el Consejo de Defensa Nacional, en adelante CODENA, MDN, Ministerio de Relaciones Exteriores, en adelante MRE, las FFMM, Ministerio del Interior, en adelante MI, Secretaria Nacional de Inteligencia en adelante SNI.

En el mismo apartado y punto en su inc. b establece, el MDN es el representante de las Fuerzas Armadas en el nivel político, es decir, le compete la parte de la protección de los intereses esenciales del Estado paraguayo y sus recursos estratégicos, que involucra a las FFMM, sea en forma disuasiva o efectiva (Ministerio de la Defensa Nacional, 2019). En tal sentido, promulga la política militar en coordinación con esta fuerza del orden, para la promoción y fortalecimiento de la ciberdefensa.

En lo que respecta al FFMM el inc. menciona que: planifica, propone y ejecuta la política militar en coordinación con el MDN, organiza, prepara y actualiza la doctrina, el personal y equipos teniendo en cuenta las amenazas tradicionales y las nuevas emergentes.

De igual manera, la política de Defensa Nacional (2019-2030) en su apartado IX «Disposiciones finales» establece:

> Esta Política Nacional de Defensa, tiene carácter obligatorio para las instituciones con responsabilidad primaria o complementaria para la Defensa Nacional, así como para aquellas de base para la Defensa de nuestros Intereses Vitales y Recursos Estratégicos. Las instituciones mencionadas deberán elaborar los planes sectoriales respectivos, contribuyentes a esta Política.
>
> Se constituye en referencia para los demás entes públicos del Estado en temas transversales de Defensa de los Intereses Vitales y Recursos Estratégicos del País (MDN, 2019, pág. 28).

Acorde a lo expuesto en los párrafos anteriores, estos lineamientos sirven de sustento para las acciones de Defensa Nacional en el ciberespacio, con proyección en la soberanía nacional

y digital, alineados con el nivel de decisión que afectan a la ciberseguridad, ciberdefensa y ciberguerra, a fin de conocer los alcances y limitaciones.

Según las políticas y doctrinas existentes de los países a nivel mundial y la región, los niveles de decisión en relación a la Defensa Nacional en el ciberespacio trasportado a la realidad nacional, comprenden:

Nivel político; política pública de ciberseguridad. Coordinado por la Presidencia de la República a través del Ministerio de Tecnologías de la Información y Comunicación en adelante MITIC y abarca a todos los sectores relacionadas a las infraestructuras tecnológicas, tecnologías de la información y comunicación del sector privado, academia, sociedad civil y público en general.

Política de ciberdefensa. Coordinado por el Comandante en Jefe y Presidente de la República a través del MDN.

Nivel estratégico operacional; ciberdefensa. A cargo del MDN, operacionalizada por el comando de las Fuerzas Militares, interactuando con el comando en jefe de las Fuerzas Armadas de la Nación; y; abarca las infraestructuras críticas.

Nivel operacional y táctico; ciberguerra. Connotación restringida al alcance interno de las Fuerzas Armadas de la Nación.

Figura 1

Niveles de decisión de defensa del ciberespacio

Fuente: Elaborado con base a la política de ciberdefensa redactada por la DIGETIC (2021) y MD 31-P-02 (2012).

Conforme a investigaciones preliminares de las políticas existentes en el mundo y especialmente en países de la región, la denominación de ciberdefensa es utilizada en planeamientos a nivel estratégico; asimismo, la ciberguerra en el operacional y táctico.

Se puede también determinar que debido a la creciente preocupación en el entorno de la seguridad internacional, por el rol fundamental de la ciberdefensa y su articulación para el sistema de Defensa Nacional, se está impulsando entre países vecinos el fortalecimiento doctrinario y la cooperación interinstitucional, por medio de foros regionales, y en esa temática Paraguay fue admitido como miembro titular del Foro Iberoamericano de Ciberdefensa, sin contar con una política definida al respecto de la ciberdefensa.

Terminologías

Amenaza cibernética. Causa potencial de un incidente no deseado, que puede provocar daños en el espacio cibernético de interés (USCCI, 2019).

Artefacto cibernético. Equipo o sistema utilizado en el ciberespacio para realizar acciones de protección, explotación y ataque cibernético (USCCI, 2019).

Activos de información. Medios de almacenamiento, transmisión y procesamiento de datos e información, el equipo necesario para esto −computadoras, equipos de comunicación e interconexión−, los sistemas utilizados son de información en general, así como los lugares donde se encuentran estos medios y las personas que tienen acceso a ellos (USCCI, 2019).

Ciberdefensa. Conjunto de acciones ofensivas, defensivas y exploratorias llevadas a cabo en el espacio cibernético, en el contexto de una planificación estratégica nacional, coordinada e integrada por el Ministerio de Defensa, con el propósito de proteger los sistemas de información de interés para la Defensa Nacional, obtener datos para la producción de conocimiento de inteligencia y comprometer los sistemas de información del oponente (USCCI, 2019).

Ciberseguridad. El arte de garantizar la existencia y continuidad de la sociedad de la información de una nación, garantizando y protegiendo, en el ciberespacio sus activos de información e infraestructura crítica (USCCI, 2019).

Ciberguerra. Corresponde al uso ofensivo y defensivo de la información y los sistemas de información para negar, explotar, corromper, degradar o destruir las capacidades de comando y control del adversario, en el contexto de la planificación militar a nivel operativo o táctico o una operación militar (USCCI, 2019).

En tal sentido, comprende las acciones que involucran herramientas de las TIC para desestabilizar o aprovechar estos métodos, sistemas de comando y control del oponente para defenderlos. Esencialmente, cubre acciones cibernéticas, así como la oportunidad para su uso o el uso efectivo será proporcional a la dependencia del oponente en las TIC (USCCI, 2019).

Cibernética. Término que se refiere a comunicación y control, actualmente relacionado con el uso de las computadoras, sistemas informáticos, redes informáticas y de comunicaciones así como su interacción (USCCI, 2019).

De manera que, en el campo de la Defensa Nacional, incluye tecnología de la información y recursos de comunicación de carácter estratégico, como los que conforman el sistema de comando y control militar, los sistemas de armas y vigilancia al igual que los sistemas administrativos que

pueden afectar las actividades operacionales (USCCI, 2019).

Dominios operacionales. El ciberespacio es uno de los cinco dominios operacionales e impregna a todos los demás, ellos son: tierra, mar, aire y espacio que son interdependientes (USCCI, 2019).

En ese entendimiento, las actividades en el ciberespacio pueden crear libertad de acción para actividades en otros dominios. También crean efectos dentro y a través del ciberespacio. El objetivo central de la integración de dominios es la disposición para aprovechar las capacidades en múltiples dominios, para crear efectos únicos y a menudo decisivos (USCCI, 2019).

Espacio cibernético. Espacio virtual compuesto de dispositivos computacionales, conectados en redes o no, donde la información digital viaja, se procesa y/o almacena (USCCI, 2019).

Infraestructura de información crítica. Un subconjunto de activos de información que afecta directamente el logro y la continuidad de la misión del Estado y la seguridad de la sociedad (USCCI, 2019).

Infraestructuras críticas. Instalaciones, servicios, bienes y sistemas que sin su rendimiento se degradan o si se interrumpen o destruyen, causarán un grave impacto social, económico, político, internacional o para la seguridad del Estado y la sociedad (USCCI, 2019).

Operación de información. Acciones coordinadas acerca del entorno de información y, llevadas a cabo con el apoyo de la inteligencia, para influir en un oponente real o potencial, reduciendo su capacidad de combate, cohesión interna y externa, así como su capacidad de toma de decisiones, para la protección del proceso de toma de decisiones en sí, contribuyendo así al logro de objetivos políticos y militares (USCCI, 2019).

Resistencia cibernética. La capacidad de mantener las infraestructuras críticas de tecnología de la información y las comunicaciones operando en condiciones de ataque cibernético o restaurarlas después de una acción adversa (USCCI, 2019).

Riesgo cibernético. Probabilidad de un incidente cibernético asociado con la magnitud del daño causado (USCCI, 2019).

Seguridad de la información y las comunicaciones (SIC). Acciones que tienen como objetivo habilitar y garantizar la disponibilidad, integridad, confidencialidad y autenticidad de los datos y la información (USCCI, 2019).

Dominio del ciberespacio

El control del ciberespacio es vital para obtener el éxito en las operaciones militares, el cual requiere de la integración de los otros dominios tradicionales como, tierra, agua, aire y espacio, con la finalidad de asegurar el empleo eficaz del ciberespacio, disponer de la libertad de acción y dificultar el acceso a personas no autorizadas.

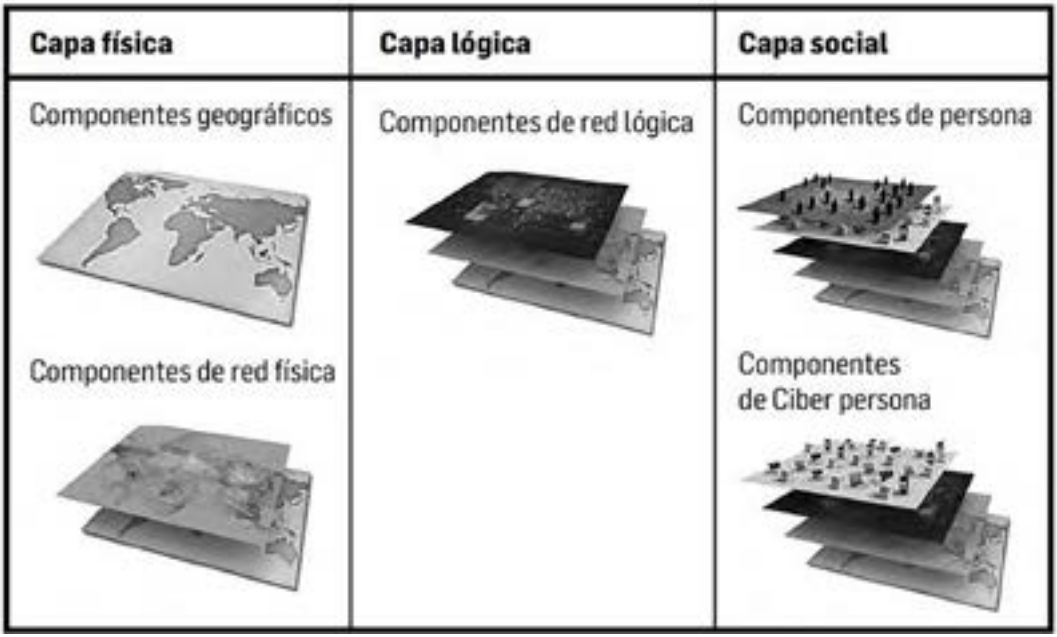
Es difícil cuantificar los daños y pérdidas que pueden generarse a través o desde el ciberespacio, pero en forma de analogía se puede poner al mismo nivel que los aviones bombarderos, con capacidad furtiva de última generación. En relación al poder relativo de combate es directamente proporcional al impacto que pueda generar ante cualquier hipótesis de conflicto.

El nuevo escenario de actuación impulsó a algunos países a fortalecer en forma proactiva la doctrina, los recursos humanos, los equipamientos e infraestructuras, a fin de mitigar las amenazas *en el ciberespacio.*

Figura 2

El ciberespacio en capas

Muy importante también es mencionar las capas de internet; se hacen referencia a *dark*



Fuente: (Cyberspace Operations Concept Capability Plan, 2010).

web o deep web −internet oculta y/o profunda−. Al respecto, el *darknet* es una red encriptada que existe de manera paralela al internet y requiere del uso de herramientas y software especiales, en tanto que la *dark web* es todo el contenido que se encuentra alojado dentro de esa red encriptada.

En ese orden de ideas, se pude decir que la mayoría de las actividades ilegales que se realiza en línea, se lleva en la *darknet,* desde la publicación de información de *login* de cuentas robadas, vulnerabilidades de seguridad informática, hasta venta de drogas, armas, municiones y explosivos.

En lo que respecta a la d*eep web* −básicamente− se refiere a cualquier sección de internet que no es accesible a los motores de búsqueda. Estas páginas no aparecen en los resultados de búsqueda, como *Google*, pero no por eso son malas o sospechosas, es la porción más grande de internet, ocupa de 400 a 550 veces el tamaño de la red superficial o *surface web* soberanía digital y la mitigación de los riesgos cibernéticos.

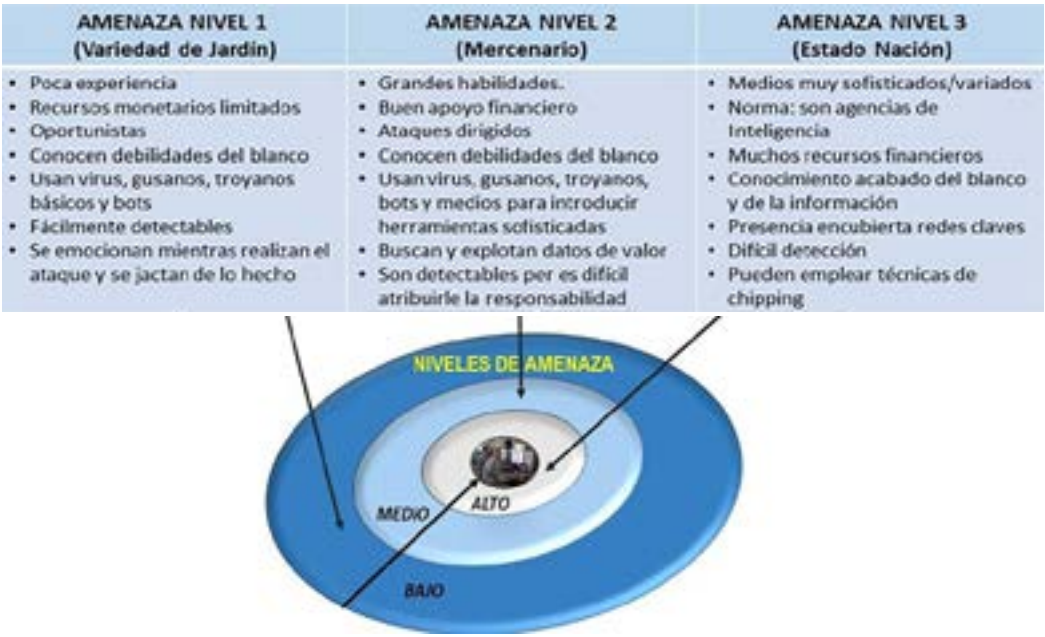
Figura 3
Internet obscura e internet profunda

Fuente: Darknet, la Dark web y el Deep webhttps://www.qore.com/ (Verificar fuente).

Figura 4
Vulnerabilidades del ciberespacio

Fuente: (Departamento de Seguridad Nacional, 2018).

Figura 5
Niveles de ciberamenazas



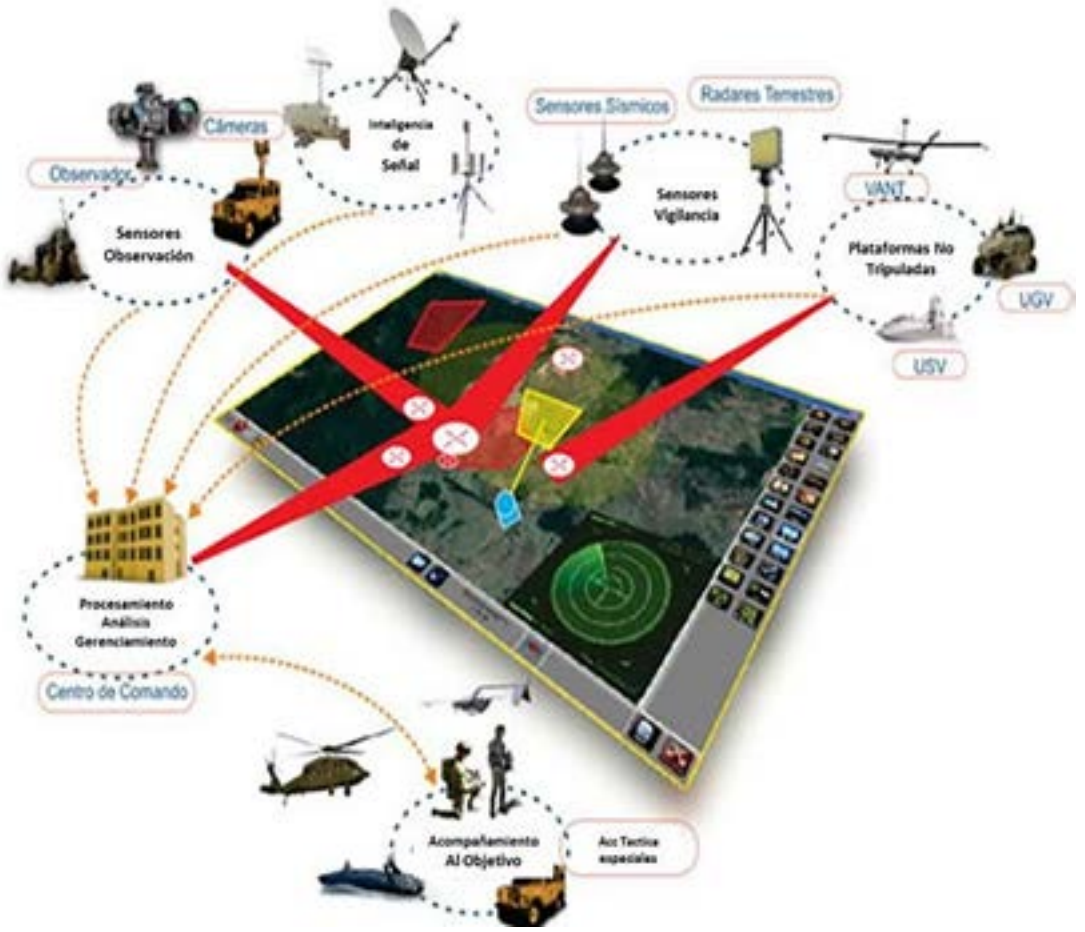
Fuente: Elaborado sobre la base del contenido de NATO.

Tabla 1
Amenazas niveles en ciberdefensa

Amenazas			
Color	**Grado**	**Descripción**	
Gris	Bajo	No afectan el ciberespacio.	Normal funcionamiento de las actividades.
Verde	Moderado	Afectan el ciberespacio, sin comprometer infraestructuras críticas de la información.	Posibilidad de ejecución de las amenazas.
Azul	Mediano	Acciones cibernéticas escalan afectando el ciberespacio, sin comprometer las infraestructuras criticas.	Aplicable cuando la percepción de la amenaza con la infraestructura critica.
Naranja	Alto	Acciones cibernéticas hostiles afectan parcialmente las infraestructuras criticas.	La infraestructura crítica fue vulnerada, pera tiene la capacidad de resiliencia.
Rojo	Muy alto	Acciones cibernéticas hostiles, exploran o niegan la disponibilidad de la infraestructura critica de la información.	La infraestructura crítica fue vulnerada y va a tardar en recuperarse.

Fuente: Elaborado sobre la base a estudios de la DIGETIC/FFAA (2021).

Figura 6
Ciberdefensa en el campo de batalla



Fuente: Presentación institucional DIGETIC/FFAA 2023

El combate moderno depende exclusivamente de obtener una potencia destacada en el ciberespacio, por medio de los equipos tecnológicos y recursos humanos acordes a las necesidades.

Tanto en las fuerzas singulares y direcciones generales, deben contar en su organización, composición y despliegue de medios de empleo para la ciberdefensa.

En esa línea, el grado de combate cibernético aumenta la potencia de combate de las fuerzas singulares y direcciones generales, dependiendo de la asimilación de los comandantes de esos escalones designados en apoyo a la Defensa Nacional a través de la ciberdefensa.

Principios de empleo de la ciberdefensa

Las operaciones militares, incluidas las llevadas a cabo en el ciberespacio, se guían por los principios derivados del estudio de campañas militares y que se enumeran en la doctrina de defensa militar. De manera que, las peculiaridades de la ciberdefensa imponen, incluso si se consideran otros principios relevantes (DIGETIC, 2021).

Principios relevantes para el uso de la ciberdefensa

Principio de efecto. Las acciones en el ciberespacio deben producir efectos que se traduzcan en ventajas estratégicas, operativas o tácticas que afecten al mundo real, incluso si estos efectos no son cibernéticos.

Principio de ocultación. Se deben tomar medidas activas para ocultarse en el ciberespacio, lo que dificulta el seguimiento de las acciones cibernéticas ofensivas y exploratorias, llevadas a cabo contra los sistemas de tecnología de la información y así como las comunicaciones del oponente. Por lo tanto, el objetivo es enmascarar la autoría y el punto de origen de estas acciones.

Principio de trazabilidad. Se deben tomar medidas efectivas para detectar acciones cibernéticas ofensivas como las exploratorias contra sistemas amigables de las TIC. En la mayoría de las veces, las acciones tomadas en el ciberespacio implican el movimiento o la manipulación de datos, que pueden registrarse en los sistemas de las TIC.

Principio de adaptabilidad. Consiste en la capacidad de ciberdefensa de adaptarse a las características cambiantes del ciberespacio, manteniendo la proactividad incluso ante cambios repentinos e impredecibles.

Características de la ciberdefensa

Al mismo tiempo de cumplir con sus principios relevantes y relacionados con la guerra, tiene las siguientes características (DIGETIC, 2021):

Inseguridad latente. Ningún sistema informático es completamente seguro por las vulnerabilidades en los activos de información, siempre serán explotadas por las amenazas cibernéticas.

Alcance global. La defensa cibernética permite realizar acciones a escala global, simultáneamente, en diferentes frentes. Un aspecto interesante en esta área de combate es que las limitaciones físicas en la distancia y el espacio, no se aplican en ciberespacio.

Vulnerabilidad de las fronteras geográficas. Las acciones de su defensa no se limitan a fronteras geográficamente definidas, ya que los agentes pueden actuar desde cualquier lugar y tener efecto en cualquier lugar.

Mutabilidad. No hay leyes de comportamiento inmutables en el ciberespacio, ya que pueden adaptarse a las condiciones ambientales y a la creatividad de los seres humanos.

Incertidumbre. Las acciones pueden no generar los efectos deseados, debido a las diversas variables que afectan el comportamiento de los sistemas computarizados.

Dualidad. Los atacantes y los administradores del sistema pueden usar las mismas herramientas para diferentes propósitos. Al respecto, los atacantes pueden usar una herramienta que busca vulnerabilidades del sistema, por ejemplo, para encontrar puntos que representen

oportunidades de ataque en sus sistemas de destino y por parte de los administradores, para descubrir las debilidades de los equipos y las redes.

Paradoja tecnológica. Cuanto más desarrollado tecnológicamente esta un sistema, más dependiendo de las TIC, en consecuencia, será más vulnerable a las acciones cibernéticas. Sin embargo, paradójicamente, este mismo oponente tendrá más condiciones para defenderse de los ciberataques, debido a su alto grado de desarrollo tecnológico.

Dilema del atacante. Duda que el atacante enfrenta al buscar o no corregir una vulnerabilidad identificada, sabiendo que la corrección hará que su defensa sea más eficiente, mientras que la no corrección aumenta su capacidad de ataque.

Función de asesoramiento. Las acciones de defensa cibernética no tienen una finalidad en sí mismas, generalmente, se utilizan para respaldar la realización de otros tipos de operaciones.

Asimetría. Basada en el desequilibrio de fuerzas, causado por la introducción de uno o más elementos de interrupción tecnológica, metodológica o procesal que pueden causar daños como los perpetrados por Estados u organizaciones con mayores condiciones económicas, por ejemplo.

Posibilidades de la ciberdefensa

Actuar en el ciberespacio. Es efectuada a través de acciones de defensa activa, defensiva y exploratoria.

Cooperar en la producción. Consiste en el conocimiento de inteligencia a través de la fuente cibernética.

Alcanzar la infraestructura. Crítica de un oponente sin limitar el alcance físico y la exposición de las tropas.

Cooperar con la ciberseguridad. Incluidos, desde organismos externos hasta el MDN, previa solicitud o en el contexto de una operación.

Cooperar con el esfuerzo de movilización. E realizada para garantizar la capacidad disuasoria de la ciberdefensa.

Obtener sorpresa. Es basado en la capacidad de explotar las vulnerabilidades de los sistemas de información del oponente.

Tomar medidas. Consiste en acciones contra oponentes más fuertes, dentro del concepto de guerra asimétrica.

Llevar a cabo acciones. Se denomina a los costos −significativamente− más bajos que las operaciones militares en otras áreas.

Limitaciones de la ciberdefensa

Capacidad limitada. Para identificar la fuente de los ciberataques.

Vulnerabilidad. Refiere a los sistemas informáticos y dificultad para identificar talentos humanos.

Gran vulnerabilidad. Las acciones de los oponentes con poder asimétrico.

Dificultad para monitorear. Los desarrollos tecnológicos en cibernética.

Posibilidad de ser sorprendido. Se da en función de las vulnerabilidades de los propios sistemas de información.

Formas de acción de la ciberdefensa

Estas pueden variar según el nivel de los objetivos −político, estratégico, operacional o táctico−, nivel de participación nacional, contexto laboral, nivel tecnológico empleado, sincronización y tiempo de preparación, como se presentará a continuación (DIGETIC, 2021):

Acción de ciberdefensa política estratégica. La acción política/estratégica se produce desde tiempos de paz, para lograr un objetivo definido al más alto nivel −generalmente− en el contexto de una operación de información o inteligencia (DIGETIC, 2021).

Acción de ciberdefensa operacional táctico. El rendimiento operacional/táctico se emplea típicamente en el contexto de una operación militar, lo que contribuye al logro del efecto deseado (DIGETIC, 2021).

Las formas de actuación de ciberdefensa. Las posibilidades de actuación y los criterios que se pueden utilizar para diferenciar las formas de actuación (DIGETIC, 2021).

Tipos de acciones de ciberdefensa

Ciberataque. Comprende acciones para interrumpir, denegar, degradar, corromper o destruir información o sistemas informáticos almacenados en la computadora, dispositivos y redes de comunicación del oponente (DIGETIC, 2021).

Protección cibernética. Cubre acciones para neutralizar ataques y explotación cibernética contra nuestros dispositivos informáticos, redes informáticas y de comunicaciones, aumentando las acciones de seguridad, defensa y guerra cibernética ante una situación de crisis o conflicto. Es una actividad permanente (DIGETIC, 2021).

Exploración cibernética. Consiste en acciones de búsqueda o recopilación, en los sistemas de tecnología de la información de interés, para obtener una conciencia situacional del entorno cibernético. Estas acciones preferiblemente deben evitar el seguimiento y sirven para generar conocimiento o identificar las vulnerabilidades de estos sistemas (DIGETIC, 2021).

Límites a las acciones de ciberdefensa

Operaciones que no son de guerra. Al realizarlas, el uso de acciones de ataque cibernético requiere autorización expresa de la autoridad competente, generalmente a nivel político (DIGETIC, 2021).

Para las acciones de explotación cibernética, deben observarse los actos normativos del sistema legal vigente. En caso de dudas, corresponde a las FF MM consultar a nivel político sobre el uso de las acciones mencionadas anteriormente.

Operaciones de guerra. Solo se realizarán las acciones efectivamente necesarias para cumplir con el punto, conforme a la decisión política-estratégica (DIGETIC, 2021).

Sistema militar de ciberdefensa

La ciberdefensa. Constituye uno de los componentes de la Defensa Nacional que es la misión constitucional de las Fuerzas Armadas, en adelante FFAA, también asignada en la política de Defensa Nacional (2019-2030). Sin embargo, las peculiaridades del espacio cibernético hacen que sea imposible cumplir esta misión, sino hay compromiso de la sociedad en su conjunto, incluido

del sentimiento de responsabilidad individual y colectiva para la protección de las infraestructuras críticas nacionales en el espacio cibernético (DIGETIC, 2021).

La efectividad de las acciones de ciberdefensa. Depende fundamentalmente del desempeño colaborativo de la sociedad paraguaya, incluidos no solo el MDN, sino también la comunidad académica, los sectores público, privado y la base de defensa industrial.

En este contexto, la necesidad de una interacción permanente entre el MDN y los otros actores externos, involucrados con el sector cibernético a nivel nacional e internacional, es de gran importancia, según lo establecido en la estrategia nacional de defensa (DIGETIC, 2021).

Las actividades de ciberdefensa en el MDN. Están orientadas a satisfacer las necesidades de la Defensa Nacional. La integración con los organismos de interés, debe buscarse desde la situación de normalidad institucional, con el fin de facilitar las acciones resultantes de una evolución a situaciones de crisis o conflicto, teniendo en cuenta el amplio espectro de estas situaciones (DIGETIC, 2021).

El sistema militar de ciberdefensa. Es un conjunto de instalaciones, equipos, doctrina, procedimientos, tecnologías, servicios y personal esenciales para llevar a cabo actividades de defensa en el ciberespacio. Asegurando conjuntamente, su uso efectivo por las FFAA, además, de prevenir u obstaculizar su uso contra los intereses de la Defensa Nacional (DIGETIC, 2021).

La ciberdefensa y la ciberseguridad

Éstas se han convertido en áreas claves de los estudios estratégicos. Su desarrollo actual coincide con el advenimiento de la sociedad de la información, las redes entre computadoras y el fenómeno −internet−, cuya expansión ha configurado la quinta dimensión de la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo global. De hecho, su estudio se convierte en una tarea obligada para la conducción político-estratégica de la defensa de las naciones (DIGETIC, 2021).

Ciberseguridad

De manera general, es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio; protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados (DIGETIC, 2021).

De manera particular, lo que permita evitar injerencias en los protocolos de los sistemas informáticos y de sus redes; lo que impida que las vulnerabilidades sean aprovechadas para atentar a los derechos de los ciudadanos e instituciones. Lo que asegure la estabilidad y buen funcionamiento de las infraestructuras (DIGETIC, 2021).

Por ello se considera el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa, a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez se impide que fuerzas enemigas los utilicen para cumplir los suyos (DIGETIC, 2021).

Tabla 2
Operaciones de ciberdefensas

Áreas de operaciones ciberdefensa (AOCD)	Operaciones de ciberdefensa
Estructura	Operaciones en la red
Terreno clave	Operaciones defensivas
Riesgos en el AOCD	Operaciones ofensivas Operaciones de vigilancia y reconocimiento

Las operaciones cibernéticas

Figura 7
Las operaciones cibernéticas

Fuente: USCCI (2019).

Método

La metodología utilizada responde a un enfoque cualitativo, con diseño no experimental. En tal sentido, el tipo es documental, de alcance descriptivo de manera que la técnica para la recolección de datos fue a través de recolección y análisis documental, los cuales fueron cargados en una ficha como instrumento para la lista de cotejos que finalmente permitió las realizar las conclusiones.

Como universo se consideró al Sistema de Defensa Nacional por medio de la Política de Defensa Nacional (2019-2030). La población está compuesta por documentos relacionados a la Política de Ciberdefensa, al respecto la muestra son las leyes dictadas por el Congreso Nacional, decretos del Poder Ejecutivo y resoluciones del MDN, así como aquellos instrumentos normativos relacionados al objeto de estudio de los siguientes países: Argentina, Perú, Chile y España, comprendidos del periodo del 2019 en adelante.

En esa línea, la investigación documental es una técnica cualitativa que selecciona y recolecta información por medio de la lectura de documentos que guardan relación con el tema de estudio, cuyas principales fuentes de información son los libros, revistas, periódicos, leyes, filmaciones, grabaciones, etc. (Ortega, 2023).

Resultados

Política de ciberdefensa comparada

Argentina

Entre los aspectos referenciales se encuentra la Resol. 2019-1380-APN-MD, A anexo 5869561, Política de ciberdefensa líneas de acción, ejes de políticas y plan para la protección de las infraestructuras críticas de interés para la defensa (Ministerio de Defensa Argentina, 2019).

Dicho anexo menciona, que a partir de conceptualizar al ciberespacio como un espacio soberano con la misión encomendada al MD de anticipar y prevenir ciberataques que pudieran comprometer la disponibilidad de los sistemas y redes de la defensa. Con ese fin se han dispuesto acciones para fortalecer las capacidades de vigilancia y control en orden a cumplimentar los objetivos de protección.

Objetivos de la misión del Ministerio en el ciberespacio

En cuanto a los objetivos de este órgano en el ciberespacio se encuentra:

- Anticipar y prevenir ataques en el ciberespacio.
- Disminuir vulnerabilidades y aumentar la resiliencia de los sistemas y redes de las TIC de las FFAA; EMCO y Mindef.
- Detectar amenazas y gestionar riesgos de ciberataques y recuperación de los sistemas e infraestructura crítica de interés para la defensa nacional.
- Adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la defensa.
- Contribuir a potenciar la base tecnológica e industrial nacional de ciberseguridad en trabajo conjunto con el Ministerio de Relaciones Exteriores y del Ministerio de Producción.
- Impulsar programas de capacitación, para superar brechas entre los recursos humanos disponibles y los demandados.

Cuatro líneas de acción para el cumplimiento de los objetivos enumerados

- LA1 Creación del Centro Nacional de Ciberdefensa.
- LA2 Proteger la disponibilidad del ciberespacio como espacio soberano.
- LA3 Reingeniería de las redes de las Fuerzas Armadas del Estado Mayor Conjunto y del

Ministerio de Defensa.

- LA4- Convergencia de las capacidades de las FFAA.

Brasil

A través del documento MD31-P-02, Política Cibernética de Defensa, el Ministerio de Defensa de la República Federativa de Brasil (2012), se establece el propósito de la Política de Defensa Cibernética, que tiene como objetivo guiar dentro del alcance del MD las actividades para dicha defensa a nivel estratégico y la guerra cibernética a nivel operativo y táctico para lograr sus objetivos.

Aplicación. A todos los componentes de la expresión militar del poder nacional, así como las entidades que pueden participar en actividades de defensa o guerra cibernética.

La definición de objetivos y la determinación de las directrices de la política de defensa cibernética obedecen a los siguientes supuestos básicos:

- La efectividad de las acciones de defensa cibernética depende fundamentalmente del desempeño colaborativo de la sociedad brasileña, incluido, no solo el MD, también la comunidad académica, los sectores público y privado y la base industrial de defensa;
- Las actividades de defensa cibernética en el MD están orientadas a satisfacer las necesidades de la defensa nacional;
- Las acciones cibernéticas ofensivas deben estar de acuerdo con la planificación preparada en respuesta a las hipótesis de empleo (HE);
- La calificación tecnológica del sector cibernético debe perseguirse de manera armoniosa con la política de la ciencia, tecnología e innovación para la defensa nacional (C,T&I);
- La efectividad de las acciones de defensa cibernética en el MD depende directamente del grado de conciencia alcanzado con las organizaciones y las personas acerca del valor de la información que poseen o procesan;
- La seguridad de la información y las comunicaciones son la base de la defensa cibernética y depende directamente de las acciones individuales; no hay defensa cibernética sin acciones de SIC; y
- Las acciones cibernéticas en el contexto del MD tienen como objetivo garantizar el uso del espacio cibernético, previniendo u obstaculizando su uso contra los intereses del país y garantizando así la libertad de acción.

Chile

En el caso de Chile a través de la Ley n.° 20424, por el cual el Ministerio de Defensa de Chile, inició el proceso de diseño de una política de defensa para temas del ciberespacio, y de la planificación de la defensa nacional en ese ámbito, a través de dos instrumentos que complementan el trabajo llevado a cabo para actualizar dichas políticas.

Al respecto, la política de ciberdefensa es parte de la política de defensa nacional, y forma parte integral de sus objetivos y principios, en especial en lo referido a: las operaciones en el ciberespacio y constituyen una dimensión específica del espectro contemporáneo del empleo de las capacidades de defensa; la planificación, conducción y ejecución de las operaciones en el ámbito se ceñirá estrictamente al respeto del derecho internacional público, con especial consideración de los derechos humanos y al derecho internacional humanitario.

Por tanto, Chile se abstendrá de recurrir a la amenaza de uso o al uso de la fuerza en una forma que contravenga el derecho internacional y podrá hacer dicho uso en legítima defensa en el ciberespacio, de conformidad con lo dispuesto en el art. 51 de la Carta de Naciones Unidas.

España

El Estado dispone de capacidades de prevención y respuesta ante las ciberamenzas, distribuidos en varios organismos, incluidos el Centro Criptográfico Nacional, las Fuerzas Armadas y el Centro de Protección de Infraestructuras Críticas.

A través del Instituto Nacional de Tecnologías de la Comunicación, se promueve el uso adecuado de los servicios que hacen posible a la sociedad de la información y la confianza en ellos (Ministerio de Defensa, 2013).

Perú

En el caso de la República del Perú, cuenta con la Ley n.° 30999 de Ciberdefensa aprobada en el año 2019, respecto a sus disposiciones general establece:

Art. 1. Objeto. La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa, dentro de su ámbito de competencia, conforme a ley.

> Art. 2. Finalidad. Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves, para mantener las capacidades nacionales frente a amenazas o ataques mediante el ciberespacio, cuando estos afecten la seguridad nacional.
>
> Art. 3. Ámbito de aplicación. Se circunscribe a la ejecución de operaciones de ciberdefensa mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional.
>
> Art. 5. Órganos ejecutores. Las Fuerzas Armadas constituidas por el Ejército, la Marina de Guerra, la Fuerza Área, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

Aspectos legales nacionales e internacionales

Tabla 3

Instrumentos normativos relacionados a la política de ciberdefensa

Instrumento normativo	Descripción
Constitución Nacional	Art. 30- De las señales de comunicación electromagnética. La emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la soberanía nacional promoverá su pleno empleo, según los derechos propios de la República y conforme con los convenios internacionales ratificados sobre la materia.
ONU, A/RES/68/243 del 27 de diciembre de 2013 aprobada por la Asamblea General, sobre la base del informe de la Primera Comisión (A/68/406).	1.Exhorta a los Estados miembros a seguir promoviendo a nivel multilateral el examen de las amenazas reales y potenciales en la esfera de la seguridad de la información y, de posibles estrategias para encarar las amenazas que surjan en esa esfera de manera compatible con la necesidad de preservar la libre circulación de la información. Invita a todos los Estados miembros a que sigan comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) La evaluación general de los temas relacionados con la seguridad de la información; b) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en ese ámbito; c) El contenido de los conceptos mencionados en el párrafo 2 supra; d) Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

Tabla 4

Instrumentos normativos relacionados a la política de ciberdefensa (continuación)

Instrumento normativo	Descripción
OEA, AG/RES.2004 (XXXIV-O/04), del 8 de junio de 2004: Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética.	Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, estableciendo lo siguiente: se declara el compromiso de identificar y combatir las amenazas terroristas emergentes, independiente de su origen o motivación, tales como las amenazas a la seguridad cibernética.
Manual de Tallin	Es considerado como el Derecho Internacional aplicable a las operaciones cibernéticas. Es la guía más completa para asesores de políticas y expertos legales sobre cómo se aplica el derecho internacional existente a las operaciones cibernéticas. Una apreciación del Manual de Tallin de la OTAN tanto estratégica como jurídica resultó necesario para encuadrar las acciones ofensivas y defensivas de actores en el ciberespacio, que fue adoptado por los países más avanzados en el área de la ciberdefensa.
Ley n.° 1.337/99 y Ley n.° 5.036/13, de Defensa Nacional y de Seguridad Interna	Art. 2. La Defensa Nacional es el sistema de políticas, procedimientos y acciones desarrollados exclusivamente por el Estado, para enfrentar cualquier forma de agresión externa e interna que ponga en peligro la soberanía, la independencia y la integridad territorial de la República, o el ordenamiento constitucional democrático vigente.
Ley n.° 6207/18 que crea el Ministerio de Tecnología de la Información y Comunicación	Art. 1° Objeto. Crear el Ministerio de Tecnologías de la Información y Comunicación (MITIC) en sustitución de la Secretaria Nacional de Tecnologías de la Información y Comunicación (SENATIC) a si como de la Secretaría de Información y Comunicación para el Desarrollo (SICOM), y establecer su carta orgánica y funciones, además de los órganos que lo conforman.
Decreto n.° 1840/14 del Poder Ejecutivo	Decreto n.°1840/14 del 1 de julio de 2014, por el que «Se declara de interés nacional la aplicación y el uso de las TIC en la gestión pública y se ordena la implementación de las unidades especializadas de las TIC».

Tabla 5

Instrumentos normativos relacionados a la política de ciberdefensa (continuación)

Instrumento normativo	Descripción
Decreto n.° 3275 que crea la DIGETIC y entes TIC en las FFMM	Por el cual se crea la Dirección General de Tecnologías de la Información y Comunicación −DIGETIC− en las FFAA de la Nación, se modifica y amplía el Decreto n.° 8792 del 22 de mayo de 2000, «por el cual se distribuye las Fuerzas Armadas de la Nación y se modifica el artículo 1º del Decreto n.° 8780/2012.
Decreto n.° 5323 del 23 de mayo del 2016	Por el cual se reglamentan los arts. 20 y 21 de la ley; n.° 4989/2013, «Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS)» y se establece la instancia de coordinación de las unidades especializadas TIC de las instituciones del Poder Ejecutivo.
Decreto n.° 7052 que crea el Plan Nacional de Ciberseguridad	Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad.
Política de Defensa Nacional 2019-2030	La finalidad de la Política de Defensa es dotar a la República del Paraguay de un eficaz instrumento de prevención y respuesta destinado a garantizar la seguridad integral y permanente de los siguientes intereses: "... la existencia del Estado paraguayo, su libertad, independencia y soberanía".

Política de ciberdefensa como colaboración a la Defensa Nacional 2019-2023

Como resultado del trabajo se presentaron los objetivos para una política de ciberdefensa contribuyentes a la Política de Defensa Nacional 2019-2030, para la protección del ciberespacio en la República del Paraguay.

Para el establecimiento de estos objetivos, fueron observados las políticas de ciberdefensa con las situaciones y condiciones particulares de los países de la región y el mundo, notando que no todos tienen el mismo nivel de ciberamenaza, mucho menos la misma capacidad en cuanto a medios y tecnología, de allí que para la formulación de los objetivos sugeridos para una política de ciberdefensa paraguaya es utilizado una guía de referencia, pero redactados con base a la realidad actual o futura del sistema de Defensa Nacional.

Lineamientos para la política de ciberdefensa

La definición y determinación de los lineamientos para esta política están orientadas a los siguientes planteamientos básicos:

En primer lugar, la ciberdefensa se encuentra a cargo del MDN y está encaminada a satisfacer las necesidades de Defensa Nacional y su proyección al mantenimiento de la soberanía digital.

De manera que, las acciones de ciberdefensa defensivas, exploratorias y defensa activa se ejecutarán de acuerdo con las hipótesis de empleo −HE− en el ciberespacio.

En ese orden de ideas, se pude afirmar que el fortalecimiento de la ciberdefensa depende primordialmente de la acción colaborativa de los actores responsables de la preservación y mantenimiento de las infraestructuras críticas, enmarcadas no solo en el ámbito del MDN, sino también su proyección a las expresiones del poder nacional.

A su vez, el fortalecimiento de la capacidad tecnológica del sector cibernético debe desarrollarse de manera que estén armonizados y articulados con la política de ciencia, tecnología e innovación para la Defensa Nacional (C, T & I).

De manera que, la optimización de acciones de la ciberdefensa dependen de las políticas, normas y procedimientos de la seguridad de la información, a través de la confidencialidad, disponibilidad e integridad de la información; así como, su cadena de custodia.

Estas acciones en el contexto de la Defensa Nacional, tienen como objetivo garantizar el uso del ciberespacio, para predecir, prevenir y obstaculizar su uso en contra de los intereses nacionales, garantizando de esta forma la libertad de acción.

En ese orden de ideas, la implementación de una arquitectura de seguridad y la redacción de normativas, a fin de crear las condiciones para el normal funcionamiento de las redes utilizadas por las infraestructuras críticas, a cargo de las FFAA de la Nación.

En esa línea, la ciberdefensa debe garantizar la continuidad de las actividades y servicios en situaciones de contingencia cibernética, para el funcionamiento de las FFAA de la Nación y su proyección a las expresiones del poder nacional.

Definir las acciones prioritarias en el ámbito de la ciberdefensa a corto, mediano y largo plazo en cuanto a: doctrina, capacitación, recursos humanos, equipamientos, infraestructura (C, T & I) infraestructuras críticas, conectividad, resiliencia y marco legal.

Objetivos

Los objetivos de la política de ciberdefensa se redactaron con base a la intención establecida en la política de Defensa Nacional de la República del Paraguay que en su presentación menciona:

> Esta Política Nacional de Defensa −PND−, fue elaborada ante la necesidad de prevenir y combatir eficientemente las nuevas amenazas; tales como el terrorismo, los secuestros, el crimen organizado transnacional, el narcotráfico, los grupos armados ilegales, los ataques cibernéticos entre otras; sin descuidar las amenazas tradicionales para la República del Paraguay (MDN, 2019, p.3).

Son objetivos de la política de ciberdefensa

- Garantizar el uso efectivo del ciberespacio a través de la ciberdefensa, para predecir, prevenir u obstaculizar las amenazas y/o riesgos emergentes que puedan surgir desde

o a través del mismo y que afecten los intereses nacionales, la soberanía nacional y su proyección a la soberanía digital.

- Proyectar y capacitar los recursos humanos necesarios con las capacidades cibernéticas, de manera a contar con las competencias necesarias, para llevar a cabo las actividades a ser desarrolladas en el ciberespacio, a cargo del MDN y a través de las Fuerzas Militares.
- Cooperar en la producción de inteligencia de fuente cibernética que sean de interés para la ciberdefensa, con énfasis en las instituciones y/o unidades responsables de la Defensa Nacional.
- Desarrollar y mantener actualizada la doctrina de empleo de la ciberdefensa.
- Adaptar las estructuras de ciencias, tecnologías e innovaciones de las fuerzas singulares y direcciones generales, para implementar las actividades de investigación y desarrollo, a fin de satisfacer las necesidades de la ciberdefensa.
- Definir los principios básicos que guían la creación de leyes y normas específicas para el empleo de la ciberdefensa.
- Contribuir a la seguridad de las infraestructuras críticas y de los activos críticos de las instituciones −públicas y privadas−, que estén fuera del alcance del MDN.
- Establecer las estrategias y las estructuras adecuadas que permitan dirigir, coordinar y supervisar las infraestructuras críticas, a cargo de las FFAA de la Nación.
- Cooperar con la movilización nacional para acciones de ciberdefensa.
- Cooperar con otros órganos o entes de ciberdefensa.

Conclusión

El ciberespacio es un nuevo escenario para la Defensa Nacional, con ambientes globales y dinámicos en el que se desenvuelven conflictos de naturaleza variada, nacionales e internacionales.

En esa línea de razonamiento, la Defensa Nacional encuentra en el ciberespacio una dimensión diferente al teatro de guerra −TG− y Teatro de Operaciones −TO− tradicional con sus campos de acción, terrestre, aérea y marítima, los cuales ya cuentan con política, doctrina, normas operativas y tácticas.

Los factores para la defensa del ciberespacio en Paraguay se están empezando a considerar y abordar. Para que sean realmente efectiva, se requiere contar con políticas, doctrinas, planificaciones y capacidades que permitan ejercer los roles propios de la Defensa Nacional en este ámbito.

Recomendación

Por ello, se recomendó tenga en consideración la idea de implementación de una −política de ciberdefensa− para prevenir y combatir eficientemente las nuevas amenazas; tales como los ataques cibernéticos, sin descuidar las amenazas tradicionales para la República del Paraguay.

Se recomendó, además a los responsables del Sistema de Defensa Nacional, iniciar el proceso para abordar la protección del ciberespacio, a través de dos acciones que complementarán el trabajo llevado a cabo, para actualizar esta política a través de la siguiente acciones:

1º. Redacción, análisis, estudio y por decreto o resolución ministerial, aprobar y divulgar una política de ciberdefensa.

2º. Dar inicio al proceso de planificación por decreto o resolución ministerial en materia de ciberdefensa, mediante la preparación de un proyecto interinstitucional que contemple la necesidad de un estamento similar al Comando Conjunto de Ciberdefensa −CCCD− con infraestructura, personal, capacitación y equipamiento.

Cabe resaltar que este trabajo de investigación que pretende la implementación de una política de ciberdefensa para el Paraguay, fue la base que sirvió para los estudios, análisis y la posterior presentación del proyecto que terminó en la redacción de la política de ciberdefensa para el Paraguay que fue aprobada por Resolución n.° 573 del 04 de octubre del 2021 por el MDN.

Referencia

Cáceres García Jairo Andrés Coronel (s. f.) (R.), Estrategia Nacional en Ciberseguridad y Ciberdefensa, Ejército de Colombia.

Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación (CONPES) 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa, Bogotá D. C., 14 de julio (2011).

Cyberspace Operations Concept Capability Plan. (22 de Febrero de 2010). irp.fas.org. Obtenido de irp.fas.org: https://irp.fas.org/doddir/army/pam525-7-8.pdf

Departamento de Seguridad Nacional. (2019 de julio de 2018). dsn.gog.es/es. Obtenido de dsn.gog.es/es: https://twitter.com/dsn/status/1023523798723833857

Ley n.º 30999/2019, Ley de Ciberdefensa, Republica del Perú.

Ley n.º 20424/2010, Ministerio de Defensa Chile, diseño de política de defensa para temas del ciberespacio.

Ministerio de la Defensa Nacional. (2019). www.mdn.gov.py. Obtenido de www.mdn.gov.py: https://www.mdn.gov.py/application/files/7415/6415/4362/Politica_de_Defensa_Nacional_2019-2030.pdf

Ministerio de la Defensa, Escuela de Altos Estudios de la Defensa. Necesidad de una conciencia nacional de Ciberseguridad. La Ciberdefensa: un reto prioritario, NIPO: 083-13-178-0 (edición papel), ISBN: 978-84-9781-862-9(edición papel), Fecha de edición: abril (2013). Barcelona – España

MD31-P-02, Política Cibernética de Defensa, Ministerio de Defensa República Federativa del Brasil, (2012).

Ministerio de la Defensa, Escuela de Altos Estudios de la Defensa. Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario, NIPO: 083-13-178-0 (edición papel), ISBN: 978-84-9781-862-9 (edición papel), Fecha de edición: abril 2013. Barcelona–España y Documentos de Seguridad y Defensa Estrategia de la información y seguridad en el ciberespacio, NIPO: 083-14-063-8, Fecha de edición: junio (2014). Barcelona–España.

Ortega, C. (6 de noviembre de 2023). www.questionpro.com/. Obtenido de www.questionpro. |com/: https://www.questionpro.com/blog/es/investigacion-documental/

Presidencia de la República España, Estrategia de Ciberseguridad Nacional, (2013).

Resolución -2019-1380-APN-MD, Anexo 5869561 Política de Ciberdefensa Líneas de Acción, ejes de políticas y plan para la Protección de las infraestructuras criticas de interés para la Defensa. Ministerio de Defensa Argentina, (2019).

Secretaría Nacional de las Tecnologías de la Información y Comunicación (SENATIC)– MITIC. Plan Nacional de Ciberseguridad.

USCCI, United States Cyber Command Instruction, Sistema de integración y desarrollo de capacidades cibernéticas. USA 2019.